

## UNITED STATES DISTRICT COURT

for the

Southern District of California

FILED

NOV 13 2014

CLERK, U.S. DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA  
BY DEPUTY

In the Matter of the Search of )

(Briefly describe the property to be searched  
or identify the person by name and address) )1 Apple Macbook Air A1370, #C02G22CADJYC, )  
FBI, 10385 Via Sorrento Pkwy, San Diego, CA )

Case No. )

'14 MJ3832

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Southern District of California (identify the person or describe property to be searched and give its location): see Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 1952, and the application is based on these facts: See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of      days (give exact ending date if more than 30 days:     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

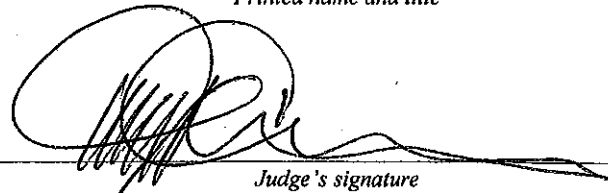


Applicant's Signature

Christopher Sedmak, SPECIAL AGENT

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/13/14


Judge's signature

City and state: San Diego, California

Hon. Karen S. Crawford, U.S. Magistrate Judge

Printed name and title

1 **A F F I D A V I T I N S U P P O R O F A P P L I C A T I O N F O R S E A R C H W A R R A N T**

2 I, Christopher J. Sedmak, being duly sworn, declare and state:

3 I

4 **INTRODUCTION AND EXPERTISE**

5 1. I have been employed as a Special Agent with the Federal Bureau of  
6 Investigation ("FBI") since September of 2002. I am currently assigned to the San  
7 Diego Field Office working as a member of the San Diego Civil Rights Squad and  
8 investigate human trafficking and other civil rights violations. I have received 16  
9 weeks of training at the FBI Academy in Quantico, Virginia and have also investigated  
10 narcotic investigations, organized crime matters, and credit fraud investigations. I  
11 have interviewed and operated informants, executed search warrants, arrested and  
12 interviewed subjects, conducted physical surveillance, utilized electronic and video  
13 surveillance, and testified in federal and state courts. I have also worked with and  
14 consulted numerous agents and law enforcement officers who have investigated  
15 human trafficking.

16 2. My experience as a Special Agent with the FBI, my participation in  
17 human trafficking investigations, my conversations with detectives with San Diego  
18 Police Department's (SDPD) Human Trafficking Unit, San Diego County Sheriff's  
19 Department (SDSD), as well as other agents and officers familiar with human  
20 trafficking, and my training form the basis of the opinions and conclusions set forth  
21 below, which I drew from the facts set forth above.

22 3. I have personally conducted the investigation that is the subject of this  
23 affidavit and I am completely familiar with the facts outlined further. This knowledge  
24 comes from personal participation in the investigation, including interviews with, and  
25 analysis of reports submitted by other law enforcement personnel participating in this  
26 investigation. However, I have not included each and every fact I know about this  
27 investigation, but only included facts to support probable cause for purposes of this  
28 search warrant.

II

**PURPOSE OF THE AFFIDAVIT**

4. This affidavit is submitted in support of an application by the United States of America for a warrant to search:

- a. One Apple Macbook Air model: A1370, serial number: C02G22CADJYC, taken from the residence of Joni Delon and currently in FBI custody.
- b. One Apple Macbook Pro model: A1398, serial number: C02LL2TEFD57, taken from the residence of Joni Deleon and currently in FBI custody.
- c. One Apple iPad Mini, model: A1455, serial number: F4KK41MHF19N, taken from the residence of Joni Deleon and currently in FBI custody.
- d. One Apple iPad Mini, model: A1432, serial number: F7NLIDHRFP84, taken from the residence of Joni Deleon and currently in FBI custody.
- e. One Apple iPad, model: A1416, serial number: DYTJ88C9DBD1, taken from the residence of Joni Deleon and currently in FBI custody.
- f. One iPod, model: A1288, serial number: 8P952WRP75J, taken from the residence of Joni Deleon and currently in FBI custody.
- g. One iPod, model: A1421, serial number: CCQM3D74DJFD, taken from the residence of Joni Deleon and currently in FBI custody.
- h. One iPhone, model: A1429, IMEI number: 990002877891646, taken from the residence of Joni Deleon and currently in FBI custody.

- i. Sony Tablet, model: SGPT11US/S, serial number: 275501000007429, taken from the residence of Joni Deleon and currently in FBI custody.
- j. Flip Video recorder, model: M2120, serial number 0S1025201103, taken from the residence of Joni Deleon and currently in FBI custody.
- k. One Seagate portable hard-drive, model: SRDOSPO, serial number: NA5P2NJB, taken from the residence of Joni Deleon and currently in FBI custody.
- l. One Verizon LG cellular telephone, model: LG-VN251SPP, serial number: 309CYHE0352889, taken from the residence of Joni Deleon and currently in FBI custody.
- m. One Verizon LG cellular telephone, model: LG-VN251SPP, serial number: 312CYHE0469481, taken from the residence of Joni Deleon and currently in FBI custody.
- n. One Verizon/Samsung cellular telephone, model: SCH-U365, MEID HEX number: A00000403DDA6C, taken from the residence of Joni Deleon and currently in FBI custody.
- o. One AT&T/Samsung cellular telephone, model: SGH-A157, serial number: R21D698R4OT, taken from the residence of Joni Deleon and currently in FBI custody.

None of the items have been reviewed by law enforcement at this time; therefore, the information relied upon to furnish the probable cause for the search of these items was not derived from the items themselves.

5. This affidavit is based upon information I gained through training and experience, as well as information relayed to me by other individuals, including other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known

1 concerning this investigation. For the reasons set forth below, I believe there is  
2 probable cause to believe that evidence relating to violations of Title 18 U.S.C. §  
3 1952 (use of facility of interstate commerce to promote prostitution) as described in  
4 Attachment B, is located in the items described in Attachment A.

### 5 III

#### 6 STATEMEN OF PROBABLE CAUSE

7 6. On June 12, 2012, Joni Razel Deleon, date of birth (DOB): 06/29/1993,  
8 was sentenced after pleading guilty to one count of California Penal Code 266i (a)(2)/  
9 664, Attempted Pandering by Encouraging. The Court found Deleon and her pimp  
10 obtained a hotel room where over the course of several days, they instructed the victim  
11 how to conduct herself as a prostitute and solicit business. Pursuant to sentencing,  
12 Deleon was placed on probation, which would be monitored by the San Diego County  
13 Probation Department, hereinafter referred to as "San Diego Probation."

14 7. On April 13, 2014, San Diego Probation conducted a Fourth Waiver  
15 search and compliance check upon Deleon at her residence, 8405 Rio San Diego Drive,  
16 Apt. 5135, San Diego, California 92108, hereinafter referred to as "the residence."

17 8. Upon arrival at the residence, San Diego Probation knocked on the front  
18 door and then heard what sounded like someone securing the lock from inside the  
19 residence. San Diego Probation continued to knock and announce their presence, but  
20 to no avail. Officers then proceeded to the rear area of the residence, where Deleon  
21 was located. Deleon claimed she could not open the door because she was in the  
22 bathroom.

23 9. A search of Deleon's residence led to the seizure of numerous items,  
24 including 21 grams of marijuana, alcohol, a 9mm Kel Tec handgun, loaded magazines,  
25 and 171 rounds of 9mm ammunition, which are violations of the terms of Deleon's  
26 probation. Further, San Diego Probation discovered personal items belonging to  
27  
28

1 Douglas Duane Evans, DOB: 01/01/1987, including, but not limited to: a California  
2 Driver's License, Credit Cards, Insurance card, and travel documents.

3 10. When questioned about Evans, Deleon indicated to San Diego Probation  
4 she did not know him. San Diego Probation then discovered two Delta airline tickets,  
5 dated March 23, destination San Francisco, in the names of Deleon and Evans. The  
6 assigned seats were 32B and 32C. I know from training and experience that  
7 traffickers, a.k.a. "pimps", are known to travel with the people they are trafficking. In  
8 this case, investigators believe Evans was travelling with Deleon of the purpose of  
9 violating 18 U.S.C. § 1952 and other state and federal offenses.

10 11. San Diego Probation also discovered numerous electronic devices, which  
11 have been listed above as items a through o. San Diego Probation believed the  
12 electronic devices were being utilized by Deleon and Evans to conduct violations of  
13 Title 18 U.S.C. §1952 by conducting telephone calls, soliciting e-mails, taking  
14 photographs, and other activities in furtherance of violations of 18 U.S.C. §1952.

15 12. As noted prior, Deleon was previously on probation for instructing a  
16 victim how to prostitute and solicit business. Law enforcement was able to identify  
17 the victim through an advertisement placed on the website Backpage.com. The report  
18 revealed, "When asked how she learned the skills for prostitution, [the victim] stated  
19 that she was taught by another prostitute known to her as "Joni", later identified as the  
20 defendant, Joni Razel Deleon." Investigators believe the electronic devices found at  
21 the residence will contain similar advertisements, photographs, and other evidence of  
22 violations of Title 18 U.S.C. §1952. Further, Deleon had previously told San Diego  
23 Probation she was unemployed, which does not explain how she was able to pay for all  
24 of the expensive electronic devices. Investigators believe the devices were purchased  
25 from the proceeds of the criminal activity.  
26  
27  
28

1       13. Deleon was arrested for the probation violations and incarcerated  
2       awaiting a hearing. San Diego Probation contacted me and provided the FBI custody  
3       of the referenced items, which were submitted into FBI evidence accordingly.  
4

5                   **BACKGROUND ON THE BUSINESS OF PROSTITUTION**  
6

7       14. Through my training, experience, and consultation with other law  
8       enforcement officers, I have learned that:

9           a. Individuals involved in illicit commercial sex<sup>1</sup> maintain records,  
10       including electronic files, related to their illicit business on computers and computer  
11       servers hosting internet applications such as electronic mail (email) and personal social  
12       networking web pages;

13          b. Individuals involved in illicit commercial sex often solicit clients  
14       through electronic advertisements and other media, such as Craig's List and  
15       backpage.com;

16          c. Individuals involved in illicit commercial sex maintain records of  
17       correspondence relating to client contact information as well as travel and lodging  
18       arrangements involved in such illegal activity;

19          d. Individuals involved in illicit commercial sex maintain documents and  
20       files containing names of associates and/or coconspirators involved in prostitution;

21          e. Individuals involved in illicit commercial sex maintain financial records,  
22       bank statements, money orders, money order receipts, and cash that are evidence of  
23       payments made in conjunction with prostitution;

24          f. Individuals involved in illicit commercial sex often maintain documents  
25       showing possession, dominion, and/or control of premises paid for by proceeds of  
26       prostitution, including utility statements, telephone statements, correspondence and  
27

---

28       <sup>1</sup> "Commercial sex act" is defined as "any sex act, on account of which anything of value is given to or received by any person. See 18 U.S.C. §1591(e)(3).



1 rental or lease agreements relating to the premises to be searched;

2 g. Individuals involved in illicit commercial sex commonly earn income in  
3 the form of cash and try to legitimize these profits. In order to do this, subjects  
4 frequently attempt to secrete, transfer, and conceal the money by means, including,  
5 but not limited to: placing assets in names other than their own to avoid detection  
6 while maintaining control; laundering the money through what appears to be  
7 legitimate businesses; hiding money in their homes, safes, and safety deposit boxes;  
8 or using the money to buy assets which are difficult to trace. Records of these and  
9 other types of transactions are often found at the residence and business fronts of  
10 individuals involved in illicit commercial sex;

11 h. Individuals involved in illicit commercial sex often operate business  
12 fronts which may appear to be legitimate, but are in fact vehicles used to conduct and  
13 promote prostitution business while avoiding detection or apprehension by law  
14 enforcement;

15 i. Many individuals involved in illicit commercial sex accept major credit  
16 cards, with the name of the business front/payee being reflected on a credit card  
17 statement as a generic entity;

18 j. Individuals involved in illicit commercial sex can keep and maintain  
19 large amounts of bulk United States currency at their residences and business fronts.  
20 Such funds are often used for everyday expenditures and to maintain and finance  
21 their ongoing illegal activity. Additionally, individuals involved in illicit  
22 commercial sex often amass and maintain assets at their residences and or business  
23 fronts which were generated by their illegal activity, or purchased with the cash  
24 earned from said illegal activity;

25 k. Individuals involved in illicit commercial sex use cellular telephones,  
26 tablets, desktop and notebook computers and maintain these items on their person  
27 and/or in their residences and/or business fronts. Individuals involved in illicit  
28



1 commercial sex use cellular telephones, tablets, and notebook computers to increase  
2 their mobility, coordinate illicit activities, and to provide pimps and prostitutes with  
3 instant access to phone calls, voice messages, text messages, instant messaging (IM)  
4 and internet based correspondence. These electronic devices allow individuals  
5 involved in illicit commercial sex to maintain contact with other pimps, prostitutes,  
6 complicit businesses, and clients. These electronic devices contain wire and  
7 electronic data concerning telephonic contact records, text messages, and electronic  
8 mail messages with co-conspirators and clients, as well as telephone books  
9 containing contact information for co-conspirators and clients. Individuals involved  
10 in illicit commercial sex also utilize digital cameras, cellular telephones, tablets,  
11 desktop and notebook computers with photograph and video capabilities to take  
12 photographs and videos of themselves as well as other coconspirators for the purpose  
13 of electronic advertising and promotion of prostitution. Moreover, I know that  
14 digital evidence can be stored on a variety of systems and storage devices including  
15 hard drives, CDs, DVDs, Ipads, Ipods, thumb drives, flash drives, and portable hard  
16 drives;

17 1. Individuals involved in illicit commercial sex often drive vehicles,  
18 sometimes rented, leased, or registered in the names of other people, to transport  
19 themselves and coconspirators, inter and intra state, to pre-arranged meetings with  
20 clients to engage in prostitution. These same individuals often get other persons to rent  
21 hotel rooms, pay for online postings or other items to avoid detection.

22 15. Based upon my experience and training, and the experience and training  
23 of other agents with whom I have communicated, the evidence of illegal activity  
24 described above in paragraph 14, subsections "a" through "l" is maintained by  
25 individuals involved in illicit commercial sex in the residence and vehicles that they  
26 and their associates live in and operate as well as on online accounts such as Facebook,  
27

1 and electronic mail accounts supported by email providers such as Yahoo!, AOL, and  
2 Apple.

3 16. Based upon the evidence in this case as set forth above, I believe that Joni  
4 Razel Deleon and Douglas Duane Evans are human traffickers and they used the  
5 referenced electronic devices to facilitate trafficking activity.

### 6 7 CELL PHONE METHODOLOGY 8

9 17. It is not possible to determine, merely by knowing the cellular  
10 telephone's make, model and serial number, the nature and types of services to which  
11 the device is subscribed and the nature of the data stored on the device. Cellular  
12 devices today can be simple cellular telephones and text message devices, can include  
13 cameras, can serve as personal digital assistants and have functions such as calendars  
14 and full address books and can be mini-computers allowing for electronic mail  
15 services, web services and rudimentary word processing. An increasing number of  
16 cellular service providers now allow for their subscribers to access their device over  
17 the internet and remotely destroy all of the data contained on the device. For that  
18 reason, the device may only be powered in a secure environment or, if possible,  
19 started in "flight mode", which disables access to the network. Unlike typical  
20 computers, many cellular telephones do not have hard drives or hard drive equivalents  
21 and store information in volatile memory within the device or in memory cards  
22 inserted into the device. Current technology provides some solutions for acquiring  
23 some of the data stored in some cellular telephone models using forensic hardware  
24 and software. Even if some of the stored information on the device may be acquired  
25 forensically, not all of the data subject to seizure may be so acquired. For devices  
26 that are not subject to forensic data acquisition or that have potentially relevant data  
27 stored that is not subject to such acquisition, the examiner must inspect the device  
28

1 manually and record the process and the results using digital photography. This  
2 process is time and labor intensive and may take weeks or longer.

3  
4 18. Following the issuance of this warrant, I submit the cellular telephones  
5 for analysis. All forensic analysis of the data contained within the telephones and  
6 their memory cards will employ search protocols directed exclusively to the  
7 identification and extraction of data within the scope of this warrant.

8  
9 19. Based on the foregoing, identifying and extracting data subject to seizure  
10 pursuant to this warrant may require a range of data analysis techniques, including  
11 manual review, and, consequently, may take weeks or months. The personnel  
12 conducting the identification and extraction of data will complete the analysis within  
13 ninety (90) days, absent further application to this court.

14 **PRIOR ATTEMPTS TO OBTAIN DATA**

15  
16 20. The United States has not attempted to obtain this data by other means  
17 except where as described above.

18 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION -**

19 **Computers**

20 21. With the approval of the Court in signing this warrant, agents executing this  
21 search warrant will employ the following procedures regarding computers and other  
22 electronic storage devices, including electronic storage media that may contain data  
23 subject to seizure pursuant to this warrant:

24 **Seizure and Retention of Instrumentalities**

- 25 a. Based upon the foregoing, there is probable cause to believe that any  
26 computers and other electronic storage devices encountered during this  
27 search are instrumentalities of the enumerated offenses because there is  
28

1 probable cause to believe that they may contain contraband and fruits of  
2 crime as provided at Rule 41(c)(2), Fed.R.Crim.P., or were used in  
3 committing crime as provided at Rule 41(c)(3). Consequently, the  
4 computers and any other electronic storage devices are subject to seizure,  
5 retention and possible forfeiture and destruction. Computers, other  
6 electronic storage devices and media confirmed onsite to contain  
7 contraband, constitute fruits of crime or to have been used to commit  
8 crime will not be returned but will be imaged offsite and analyzed as  
9 provided beginning at subparagraph (c) below. The onsite confirmation  
10 may be provided by an owner or user of the computer or storage device or,  
11 if feasible, may be obtained by conducting a limited onsite forensic  
12 examination to determine if the subject media contains any contraband or  
13 otherwise is an instrumentality. Computers and other electronic storage  
14 devices and media that are not confirmed onsite as instrumentalities will  
15 be taken offsite for imaging and preliminary analysis in accordance with  
16 subparagraph (b) below.

- 17  
18 b. The offsite imaging and preliminary analysis of computers, other  
19 electronic storage devices and media to confirm their status as  
20 instrumentalities will be conducted within forty-five (45) days of seizure.  
21 Seized items confirmed to be instrumentalities will not be returned and  
22 will be further analyzed as provided below. If the preliminary analysis,  
23 by definition an incomplete or partial analysis, does not confirm that a  
24 seized item is an instrumentality, the original item will be returned  
25 promptly to its owner, absent an extension of time obtained from the  
26 owner or from the court. An image of the items will be retained and  
27 subjected to a complete forensic analysis, as provided below.  
28

- 1  
2 c. Computers and other electronic storage devices and media that are  
3 retained as instrumentalities will not be returned to its owner. The owner  
4 will be provided the name and address of a responsible official to whom  
5 the owner may apply in writing for return of specific data not otherwise  
6 subject to seizure for which the owner has a specific need. The identified  
7 official or other representative of the seizing agency will reply in writing.  
8 In the event that the owner's request is granted, arrangements will be  
9 made for a copy of the requested data to be obtained by the owner. If the  
10 request is denied, the owner will be directed to Rule 41(g), Federal Rules  
11 of Criminal Procedure.  
12

13 **Identification and Extraction of Relevant Data**

- 14 d. A forensic image is an exact physical copy of the hard drive or other  
15 media. After obtaining a forensic image, the data will be analyzed to  
16 identify and extract data subject to seizure pursuant to this warrant.  
17 Analysis of the data following the creation of the forensic image can be a  
18 highly technical process requiring specific expertise, equipment and  
19 software. There are literally thousands of different hardware items and  
20 software programs, and different versions of the same program, that can  
21 be commercially purchased, installed and custom-configured on a user's  
22 computer system. Computers are easily customized by their users.  
23 Even apparently identical computers in an office environment can be  
24 significantly different with respect to configuration, including  
25 permissions and access rights, passwords, data storage and security. It is  
26 not unusual for a computer forensic examiner to have to obtain  
27 specialized hardware or software, and train with it, in order to view and  
28

1 analyze imaged data.

2  
3 e. Analyzing the contents of a computer or other electronic storage device,  
4 even without significant technical issues, can be very challenging.  
5 Searching by keywords, for example, often yields many thousands of hits,  
6 each of which must be reviewed in its context by the examiner to  
7 determine whether the data is within the scope of the warrant. Merely  
8 finding a relevant hit does not end the review process. The computer  
9 may have stored information about the data at issue: who created it,  
10 when and how it was created or downloaded or copied, when was it last  
11 accessed, when was it last modified, when was it last printed and when it  
12 was deleted. Sometimes it is possible to recover an entire document that  
13 never was saved to the hard drive if the document was printed.  
14 Moreover, certain file formats do not lend themselves to keyword  
15 searches. Keywords search text. Many common electronic mail,  
16 database and spreadsheet applications do not store data as searchable text.  
17 The data is saved in a proprietary non-text format. Documents printed by  
18 the computer, even if the document never was saved to the hard drive, are  
19 recoverable by forensic programs but not discoverable by keyword  
20 searches because the printed document is stored by the computer as a  
21 graphic image and not as text. Similarly, faxes sent to the computer are  
22 stored as graphic images and not as text. In addition, a particular  
23 relevant piece of data does not exist in a vacuum. To determine who  
24 created, modified, copied, downloaded, transferred, communicated about,  
25 deleted or printed the data requires a search of other events that occurred  
26 on the computer in the time periods surrounding activity regarding the  
27 relevant data. Information about which user had logged in, whether  
28

1 users share passwords, whether the computer was connected to other  
2 computers or networks, and whether the user accessed or used other  
3 programs or services in the time period surrounding events with the  
4 relevant data can help determine who was sitting at the keyboard.

5  
6 f. It is often difficult or impossible to determine the identity of the person  
7 using the computer when incriminating data has been created, modified,  
8 accessed, deleted, printed, copied, uploaded or downloaded solely by  
9 reviewing the incriminating data. Computers generate substantial  
10 information about data and about users which generally is not visible to  
11 users. Computer-generated data, including registry information,  
12 computer logs, user profiles and passwords, web-browsing history,  
13 cookies and application and operating system metadata, often provides  
14 evidence of who was using the computer at a relevant time. In  
15 addition, evidence such as electronic mail, chat sessions, photographs and  
16 videos, calendars and address books stored on the computer may identify  
17 the user at a particular, relevant time. The manner in which the user has  
18 structured and named files, run or accessed particular applications, and  
19 created or accessed other, non-incriminating files or documents, may  
20 serve to identify a particular user. For example, if an incriminating  
21 document is found on the computer but attribution is an issue, other  
22 documents or files created around that same time may provide  
23 circumstantial evidence of the identity of the user that created the  
24 incriminating document.

25  
26 g. Analyzing data has become increasingly time-consuming as the volume  
27 of data stored on a typical computer system and available storage devices  
28



1 has become mind-boggling. For example, a single megabyte of storage  
2 space is roughly equivalent of 500 double-spaced pages of text. A single  
3 gigabyte of storage space, or 1,000 megabytes, is roughly equivalent of  
4 500,000 double-spaced pages of text. Computer hard drives are now  
5 being sold for personal computers capable of storing up to 2 terabytes  
6 (2,000 gigabytes) of data. And, this data may be stored in a variety of  
7 formats or encrypted (several new commercially available operating  
8 systems provide for automatic encryption of data upon shutdown of the  
9 computer). The sheer volume of data also has extended the time that it  
10 takes to analyze data. Running keyword searches takes longer and  
11 results in more hits that must be individually examined for relevance.  
12 And, once reviewed, relevant data leads to new keywords and new  
13 avenues for identifying data subject to seizure pursuant to the warrant.  
14

15 h. Based on the foregoing, identifying and extracting data subject to seizure  
16 pursuant to this warrant may require a range of data analysis techniques,  
17 including the use of hashing tools to identify evidence subject to seizure  
18 pursuant to this warrant, and to exclude certain data from analysis, such as  
19 known operating system and application files. The identification and  
20 extraction process may take weeks or months. The personnel conducting  
21 the identification and extraction of data will complete the analysis within  
22 one-hundred twenty days (120) from seizure pursuant to this warrant,  
23 absent further application to this court.  
24

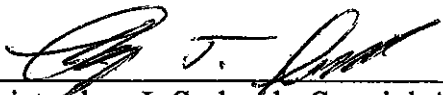
25 i. All forensic analysis of the imaged data will employ search protocols  
26 directed exclusively to the identification and extraction of data within the scope of this  
27 warrant.  
28

1  
2  
3 **GENUINE RISKS OF DESTRUCTION**  
4

5 22. Based upon my experience and training, and the experience and training  
6 of other agents with whom I have communicated, electronically stored data can be  
7 permanently deleted or modified by users possessing basic computer skills. In this  
8 case, there is no genuine risk of destruction of evidence as the items are in law  
9 enforcement custody.  
10

11 **CONCLUSION**  
12

13 23. Based upon the foregoing, I believe there is probable cause to believe the  
14 items identified in Attachment B have been used in the commission of a crime and  
15 constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1952 and  
16 will be found in the items to be searched as provided in Attachment A.  
17

18   
19 Christopher J. Sedmak, Special Agent, FBI

20 Subscribed and sworn to before me  
21 this 13<sup>th</sup> day of November, 2014.

22   
23  
24 United States Magistrate Judge

25 **KAREN S. CRAWFORD**  
26  
27  
28

**ATTACHMENT A**

- 1
- 2
- 3 One Apple Macbook Air model: A1370, serial number: C02G22CADJYC.
- 4 One Apple Macbook Pro model: A1398, serial number: C02LL2TEFD57.
- 5 One Apple iPad Mini, model: A1455, serial number: F4KK41MHF19N.
- 6 One Apple iPad Mini, model: A1432, serial number: F7NLIDHRFP84.
- 7 One Apple iPad, model: A1416, serial number: DYTJ88C9DBD1.
- 8 One iPod, model: A1288, serial number: 8P952WRP75J.
- 9 One iPod, model: A1421, serial number: CCQM3D74DJFD.
- 10 One iPhone, model: A1429, IMEI number: 990002877891646.
- 11 Sony Tablet, model: SGPT11US/S, serial number: 275501000007429.
- 12 Flip Video recorder, model: M2120, serial number 0S1025201103.
- 13 One Seagate portable hard-drive, model: SRDOSPO, serial number: NA5P2NJB,
- 14 taken from the residence of Joni Deleon and currently in FBI custody.
- 15 One Verizon LG cellular telephone, model: LG-VN251SPP, serial number:
- 16 309CYHE0352889.
- 17 One Verizon LG cellular telephone, model: LG-VN251SPP, serial number:
- 18 312CYHE0469481.
- 19 One Verizon/Samsung cellular telephone, model: SCH-U365, MEID HEX number:
- 20 A00000403DDA6C.
- 21 One AT&T/Samsung cellular telephone, model: SGH-A157, serial number:
- 22 R21D698R4OT.
- 23 All items are located at FBI, 10385 Via Sorrento Parkway, San Diego, CA 92121.
- 24
- 25
- 26
- 27
- 28

**ATTACHMENT B**

**For any computers or computer media:** Authorization is sought to search for and seize evidence that relates to the violation of Title 18, United States Code, Section 1952. This authorization includes the search of physical documents and includes electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the "Procedures For Electronically Stored Information" provided in the affidavit submitted in support of this warrant. Items to be seized include the following:

a. User-attribution data to include data reflecting who used or controlled any computer or electronic storage device at or around the time that data reflecting criminal activity within the scope of this warrant was created, accessed, deleted, modified, copied, downloaded, uploaded or printed. User-attribution data includes registry information, computer logs, user profiles and passwords, web-browsing history, cookies, electronic mail stored on the computer or device, electronic address books, calendars, instant messaging logs, electronically-stored photographs and video, file structure and user-created documents, including metadata.

b. Information or correspondence in any form pertaining to the prostitution, or attempted prostitution, of any person to engage in a commercial sex acts as defined by 18 U.S.C. §1591 in violation of 18 U.S.C. § 1952, that were transmitted or received, including by computer, or some other facility or means of interstate or foreign commerce, including other correspondence such as electronic mail, chat logs, and electronic messages.

c. Electronically stored communications, images or messages reflecting computer on-line communications, instant messages, and/or e-mail messages that reference, discuss commercial sex acts as defined by 18 U.S.C. §1591.

d. Electronic communications and/or attachments (sent, saved or received) coercing or enticing or discussing commercial sex acts as defined by 18 U.S.C. §1591.

e. Electronic mail and attachments that provide context to any electronic mail reflecting the criminal activity described in this warrant including any electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail that identifies any users of the subject account.

**For any cellular telephone devices and any storage devices,** such as SIM cards or flash memory devices attached to, inserted in or seized with the device, will be analyzed and the following data will be seized only to the extent that it contains or

1 depicts evidence of violations of Title 18, United States Code, Section 1952,  
2 including evidence reflecting use, dominion and control of the device such as  
3 communications, records or data including but not limited to emails, text messages,  
4 photographs, audio files, videos, or location data:

- 5 1. tending to indicate efforts to persuade, induce, entice or coerce a person to  
6 travel interstate to engage in prostitution;
- 7 2. tending to show efforts to solicit commercial sex acts on websites including  
8 but not limited to Backpage.com;
- 9 3. tending to indicate interstate travel for the purposes of engaging in, or  
10 assisting others to engage in, commercial sex activity;
- 11 4. tending to identify other facilities, stage devices, or services-such as email  
12 addresses, IP addresses, phone numbers-that may contain electronic evidence  
13 tending to show efforts to persuade, induce, entice or coerce a person to travel  
14 interstate to engage in prostitution;
- 15 5. tending to identify co-conspirators, criminal associates, or other involved in  
16 promoting prostitution in violation of 18 U.S.C. § 1952;
- 17 6. Web-browsing history and any stored web pages relating to 18 U.S.C.  
18 §1952;
- 19 7. tending to identify travel to or presence at locations used for commercial sex  
20 acts;
- 21 8. tending to identify the user of, or persons with control over or access to, the  
22 subject phone;
- 23 9. tending to establish a pimp/prostitute relationship between and among  
24 individuals; or
- 25 10. tending to place in context, identify the creator or recipient of, or establish  
26 the time of creation or receipt of communications, records, or data above.
- 27
- 28